

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Internet Information Services (IIS)

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-215>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2009-AVI-215 |
| Titre | Vulnérabilités dans Internet Information Services (IIS) |
| Date de la première version | 10 juin 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS09-020 du 09 juin 2009 |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Internet Information Services 5.0 ;
- Microsoft Internet Information Services 5.1 ;
- Microsoft Internet Information Services 6.0.

3 Résumé

Des vulnérabilités ont été identifiées dans le serveur Web Microsoft Internet Information Services utilisé avec WebDAV. L'une d'elle a fait l'objet de l'alerte CERTA-2009-ALE-007.

L'exploitation par le biais de requêtes spécialement construites permet à une personne distante d'élever ses privilèges et de contourner des phases d'authentification mises en place.

4 Description

Des vulnérabilités ont été identifiées dans le serveur Web Microsoft Internet Information Services utilisé avec WebDAV. L'une d'elle a fait l'objet de l'alerte CERTA-2009-ALE-007.

L'exploitation par le biais de requêtes spécialement construites permet à une personne distante d'élever ses privilèges et de contourner des phases d'authentification mises en place.

5 Solution

Se référer au bulletin de sécurité Microsoft MS09-020 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Alerte CERTA-2009-ALE-007 du 18 mai 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-007/>
- Bulletin de sécurité Microsoft MS09-020 du 09 juin 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-020.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-020.msp>
- Référence CVE CVE-2009-1122 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1122>
- Référence CVE CVE-2009-1535 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1535>
- Référence CVE CVE-2009-1676 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1676>

Gestion détaillée du document

10 juin 2009 version initiale.